

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

A certain cellular phone seized
during the arrest of Mubarik Ibrahim
on January 17, 2023

Case No. 2:23-mj-66

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 18 USC 1956(h)
 18 USC 1956(a)(1)(B)(i)
 18 USC 1956(a)(2)(B)(i)
 18 USC 1343

Money Laundering Conspiracy
 Money Laundering
 Money Laundering
 Wire Fraud

Offense Description

The application is based on these facts:

See attached affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Shawn A. Mincks

Applicant's signature

Shawn Mincks, Special Agent, IRS-CI

Printed name and title

Sworn to before me and signed in my presence.

Date: 2/2/2023

City and state: Columbus, OH

Chelsey M. Vascara

Chelsey M. Vascara
 United States Magistrate Judge

Judge's signature

Chelsey M. Vascara, U.S. Magistrate Judge

Printed name and title

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

**AFFIDAVIT
IN SUPPORT OF SEARCH WARRANT**

I, Shawn Mincks, Special Agent, U.S. Department of the Treasury, Internal Revenue Service, Criminal Investigation, being duly sworn, depose and say that:

Introduction and Purpose

1. I am a Special Agent with IRS-Criminal Investigation and have been so employed since 2008. I have received specialized law enforcement training at the Federal Law Enforcement Training Center, Glynco, Georgia and additional specialized training from the IRS. My duties as a Special Agent include conducting investigations of individuals and businesses that have violated Federal Law, particularly those laws found under Title 18, Title 26 and Title 31 of the United States Code. I have participated in multiple such investigations, including several investigations related to individuals who launder funds derived from romance and other international fraud schemes.

2. I am assigned to pursue a federal criminal investigation of Mubarik Ibrahim. I make this affidavit in support of a search warrant for a cellular phone seized by IRS-Criminal Investigation during the arrest of Mubarik Ibrahim on January 17, 2023. The items is further described as the following and is also described in Attachment A:

Attachment A

- a. Red Apple iPhone cell phone seized during the execution of an arrest warrant on Mubarik Ibrahim

3. The device is currently in the possession of IRS-CI located at 401 North Front Street, Suite 375, Columbus, Ohio.

4. The information in this affidavit is either personally known to me based upon my experience, investigative activities, and analysis of records and interviews; or it has been relayed to me by other agents and/or law enforcement personnel. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact know to me concerning the investigation. I have set forth only the facts I believe are necessary to support the requested search warrant.

5. I contend there is probable cause to believe that Ibrahim has been involved in a conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h), since at least December 2014 and committed or caused to be committed multiple acts in violation of 18 U.S.C. § 1956(a)(1)(B)(i) and 18 U.S.C. § 1956(a)(2)(B)(i). I further contend that evidence of such violations and evidence of wire fraud, in violation of 18 U.S.C. § 1343, is located on or in the item described in paragraph #2 and in Attachment A.

6. Through interviews and analysis of financial records and other documentation, I believe the investigation to date tends to show that parties known to Ibrahim have defrauded numerous individuals throughout the United States and the world through so-called "romance" and/or other fraud schemes. Furthermore, Ibrahim knowingly and willfully facilitated the receipt, concealment and transfer of funds derived from the victims of these schemes.

7. Through investigative experience I know that perpetrators of romance scams post fake profiles on various dating or social media websites, then individuals throughout the United States and the world are contacted by or enticed to initiate contact with the perpetrators. After contacting the victims online, the perpetrators use email, instant messaging services, text messaging, various smart phone applications and phone calls to build a relationship of trust with the victims. Once trust is gained, the perpetrators convince the victims to provide money for various purported reasons, all of which are untrue. The perpetrators tell many of the victims that they are overseas. The victims then wire transfer, direct transfer or deposit money into bank accounts within the United States. The bank account holders in the United States then transfer the fraudulently obtained funds to the scammers in myriad ways.

8. Evidence shows that Ibrahim controlled some of the accounts into which victim funds were deposited. The victims provided the funds with the expectation that the money would be used to assist their online "friend."

9. Contemporaneous with and subsequent to the receipt of victim funds, Ibrahim disposed of the money through cash withdrawals; international and domestic wire transfers to his co-conspirators; issuances of personal checks; purchases of official checks; and personal expenditures. The loss to all victims from whom Ibrahim received funds exceeds \$750,000.

10. The affiant believes that evidence garnered so far in the investigation tends to show that Ibrahim knew that the funds he was receiving were derived from some kind of unlawful activity. The evidence further shows that the funds were, in fact, derived from a specified unlawful activity, namely wire fraud (18 U.S.C. § 1343). From the recipient accounts, the funds were not used in the manner promised to the victims of the fraud. Instead, the funds were used in financial transactions designed to conceal the nature, location, source, ownership and control of the funds, in violation of 18 U.S.C. § 1956 (a)(1)(B)(i). Many of the transactions designed to conceal the nature, location, source, ownership and control of the funds were conducted internationally, in violation of 18 U.S.C. § 1956 (a)(2)(B)(i).

11. On January 12, 2023, the affiant submitted an Affidavit in Support of Criminal Complaint alleging the activities described in paragraph #10 and detailed in the following paragraphs. As a result, Ibrahim was charged via Criminal Complaint with the alleged money laundering activities and an arrest warrant was issued. On January 17, 2023, Special Agents with IRS-Criminal Investigation arrested Ibrahim at his residence. Ibrahim's wife was present at the time of the arrest. Immediately after Ibrahim was taken into custody, Special Agents with IRS-Criminal Investigation asked Ibrahim's wife to gather warmer clothing for Ibrahim and Ibrahim's cell phone. She provided the clothing and the cell phone to Special Agents with IRS-Criminal

Investigation. Special Agents with IRS-Criminal Investigation seized the phone to preserve evidence pending application for a search warrant by the affiant.

Witness Statements and Bank Account Transactions

12. According to an interview with Person 1, whose identity is known to the affiant, Person 1 met somebody she believed to be named Dennis Williams on a dating website sometime in 2014. Williams told Person 1 that somebody he trusted had tried to steal some gold he owned, and the gold had made its way to England. Williams told Person 1 that he needed money to pay for various fees related to retrieval of the gold, including attorney fees and taxes. Williams promised to give Person 1 a portion of gold in return for her payment of the fees. Person 1's granddaughter eventually discovered that Williams was not a real person.

13. Bank records show that, on December 26, 2014, Person 1 transferred \$12,000 into JP Morgan Chase Bank account # xx3783. Ibrahim had opened the account on November 7, 2014 and was the only signer on the account. The funds were commingled with funds from other sources. Using the commingled funds, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds, including cash withdrawals totaling at least \$11,400.

14. According to an interview with Person 2, whose identity is known to the affiant, Person 2 met somebody she believed to be named Samuel George on social media in 2016. George told Person 2 that he was in the army and serving in Iraq. Eventually, George asked Person 2 to send him money for various reasons, including to pay storage fees related to gold bars. Person 2 sent what she estimated to be \$50,000 to various people at George's request.

15. Bank records show that on March 7, 2016, Person 2 wired \$4,000 to Huntington Bank account # xx3631. Ibrahim had opened the account on June 18, 2015 and was the only signer on the account. The funds were commingled with funds from other sources. Using the commingled funds, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Ibrahim simultaneously transmitted the proceeds of wire fraud to a place outside the United States, and the transactions were designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Specifically, Ibrahim sent two transfers of \$2,004.99 each, including fees, on March 8, 2016 and March 9, 2016 to Conspirator 1 in Tamale, Ghana via World Remit, an international money servicing business.

16. According to an interview with Person 3, whose identity is known to the affiant, Person 3 met somebody he believed to be named Linda Brown on social media and developed a relationship. After initial contact, Person 3 also communicated with Brown via email. Brown told Person 3 that she was from the United States, but she had travelled to London where she had a gold consignment. Brown told Person 3 that there would be a \$600,000 fee to sell the gold and asked Person 3 to assist with paying the fee. Person 3 sent money to various people at Brown's direction.

17. According to an interview with Person 4, whose identity is known to the affiant, Person 4

met somebody she believed to be named James Gibson on the internet. Gibson told Person 4 that he was in the military and serving in Afghanistan. Gibson eventually asked Person 4 to send him money to pay fees associated with transporting a shipment of gold back to the United States. Person 4 sent approximately \$50,000 at Gibson's direction in relation to the alleged package before realizing she had been defrauded.

18. According to an interview with Person 5, whose identity is known to the affiant, Person 5 met somebody she believed to be named Walker Michael on social media. Michael told Person 5 he was in the military. Eventually, Michael asked Person 5 to send him money to assist with expenses related to his adopted son and the shipment of a package of valuable assets. Person 5 eventually realized she had been defrauded when she found Michael's pictures on a website dedicated to revealing fraudsters.

19. Bank records show that between July 8, 2016 and October 7, 2016, funds from Person 3 totaling \$52,000; funds from Person 4 totaling \$50,000; and funds from Person 5 totaling \$5,000 were deposited into Huntington Bank account # xx4490. Signatures on the backs of the cashier's checks received from Person 3 and Person 5 appear to match Ibrahim's signature on the signature card for Huntington Bank account # xx4490. Ibrahim had opened the account on June 26, 2015 and was the only signer on the account. The \$105,000 received from Persons 3, 4 and 5 was commingled with funds from other sources. Using the commingled funds, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds, including cash withdrawals totaling at least \$59,000; wires to a third party totaling \$22,000; and a cashier's check issued to an online automobile auction company in the amount of \$15,409.

20. World Remit, Western Union and MoneyGram (all of which are money servicing businesses) records show that Ibrahim transmitted the proceeds of wire fraud to a place outside the United States, and such transactions were designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Specifically, Ibrahim transferred funds to individuals in Ghana, including Conspirator 1, who received \$2,900; Conspirator 2, who received \$4,800; Conspirator 3, who received \$3,380; and Conspirator 4, who received \$13,963.

21. Bank records show that on June 16 and June 29, 2017, checks issued by Person 3 in the amounts of \$30,000 and \$2,000, respectively, were deposited into US Bank account # xx4710. Ibrahim had opened the account on September 26, 2016 and was the only signer on the account. The funds were commingled with funds from other sources. Using the commingled funds, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds including wire transfers via World Remit totaling at least \$7,353.27; a check issued to a third party in the amount of \$23,100; and cash withdrawals totaling \$1,530.

22. World Remit records show that Ibrahim transmitted the proceeds of wire fraud to a place outside the United States, and such transactions were designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Specifically, Ibrahim transferred funds to individuals in Ghana, including Conspirator 1, who received \$700; Conspirator 2, who received \$2,000; Conspirator 3, who received \$2,000; and Conspirator 4, who received \$1,600.

23. According to an interview with Person 6, whose identity is known to the affiant, Person 6 met somebody she believed to be named Mark Johnson on social media in November 2016. Johnson told Person 6 he was serving in the military in Afghanistan, and Person 6 and Johnson became "pen pals." Johnson eventually told Person 6 that he needed money to fly home to the United States. After Person 6 agreed to help, Johnson instructed Person 6 to mail money orders and send other funds. Person 6 estimates that she sent approximately \$75,000 to various recipients at Johnson's request before Person 6's daughter convinced her that she had been defrauded.

24. Bank records show that, on February 21, 2017, two cashier's checks remitted by Person 6 in the amounts of \$1,500 each were deposited into US Bank account # xx4710. The signatures on the backs of the cashier's checks appear to match signatures on checks issued by Ibrahim from US Bank account # xx4710. The funds were commingled with funds from other sources. Using the commingled funds, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds including wire transfers to third parties via World Remit totaling \$5,354.99.

25. World Remit records show that Ibrahim transmitted the proceeds of wire fraud to a place outside the United States, and such transactions were designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Specifically, Ibrahim transferred \$5,000 to Conspirator 2 in Tamale, Ghana.

26. Bank records show that, on February 21, 2017, three U.S. Postal money orders remitted by Person 6 in the amounts of \$1,000 each and on which memoranda read "For Mark Johnson" were deposited into Huntington Bank account # xx4490. The signatures on the backs of the money orders appear to match Ibrahim's signature on the signature card for Huntington Bank account # xx4490. The funds were commingled with funds from other sources. Using the commingled funds, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds by making cash withdrawals totaling at least \$4,300.

27. According to an interview with Person 8, whose identity is known to the affiant, Person 8 was randomly contacted on social media in 2018 by somebody she believed to be named Raymond George. George told Person 8 he was from Florida and was in the army. At one point, George told Person 8 he was in Canada. Another time, he told Person 8 he was in Amsterdam. George asked Person 8 to send him money to assist him returning home.

28. Bank records show that between May 29, 2018 and September 7, 2018, Person 8 wired \$105,900 to Ibrahim at Huntington Bank account # xx5884. Ibrahim had opened the account on March 15, 2018 and was the only signer. The funds received from Person 8 were commingled in the account with funds from other sources. Using the commingled funds on or about the dates set forth below, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Simultaneously, Ibrahim transmitted the proceeds of wire fraud to a place outside the United States and such transactions were designed to conceal or disguise the nature, location, source,

ownership, or control of the proceeds:

- a. May 31, 2018 - \$959.99, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- b. June 11, 2018 - \$2,324.51, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- c. June 26, 2018 - \$1,158.79, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- d. July 6, 2018 - \$746.49, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- e. July 9, 2018 - \$1,995.59, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- f. July 19, 2018 - \$1,903.39, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- g. July 30, 2018 - \$2,180.01, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- h. July 31, 2018 - \$3,284.01, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- i. August 1, 2018 - \$2,181.21, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- j. August 6, 2018 - \$135.00, including fees, via Wave to Conspirator 3, which was received in Ghanaian currency (Cedis)
- k. August 6, 2018 - \$2,617.56, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- l. August 7, 2018 - \$265.00, including fees, via Wave to Conspirator 3, which was received in Ghanaian Cedis
- m. August 9, 2018 - \$1,543.09, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- n. August 13, 2018 - \$365.00, including fees, via Wave to Conspirator 3, which was received in Ghanaian Cedis
- o. August 14, 2018 - \$3,271.01, including fees, via World Remit to Conspirator 3 in Tamale, Ghana

- p. August 15, 2018 - \$2,304.01, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- q. August 15, 2018 - \$437.00, including fees, via Wave to Conspirator 3, which was received in Ghanaian Cedis
- r. August 17, 2018 - \$3,275.51, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- s. August 20, 2018 - \$2,620.51, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- t. August 21, 2018 - \$3,053.51, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- u. August 24, 2018 - \$3,253.54, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- v. August 28, 2018 - \$3,281.59, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- w. September 10, 2018 - \$1,205.91, including fees, via World Remit to Conspirator 5 in Tamale, Ghana
- x. September 10, 2018 - \$107.76, including fees, via Wave to Conspirator 3, which was received in Ghanaian Cedis
- y. September 11, 2018 - \$517.50, including fees, via Wave to Conspirator 3, which was received in Ghanaian Cedis
- z. September 13, 2018 - \$107.30, including fees, via Wave to Conspirator 3, which was received in Ghanaian Cedis
- aa. September 13, 2018 - \$3,249.41, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- bb. September 13, 2018 - \$1,093.13, including fees, via World Remit to Conspirator 5 in Tamale, Ghana
- cc. September 17, 2018 - \$3,243.77, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- dd. September 17, 2018 - \$3,229.81, including fees, via World Remit to Conspirator 6 in Tamale, Ghana

29. According to an interview with Person 9, whose identity is known to the affiant, someone randomly contacted Person 9 by text and asked for money to help pay for schooling for a girl because her parents had been killed in a wreck. Person 9 thought it sounded legitimate because he was instructed to send money to a Huntington Bank account. Person 9 had also previously sent money to a girl he met on an online dating website. Person 9 often receives texts and calls requesting money from him/her, and he never knows if its legitimate or not.

30. Bank records show that on September 24, 2018, Person 9 wired \$5,000 to Ibrahim at Huntington Bank account # xx5884. The funds received from Person 9 were commingled with funds from other sources. Using the commingled funds on or about the date set forth below, Ibrahim engaged in a financial transaction involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Simultaneously, Ibrahim transmitted the proceeds of wire fraud to a place outside the United States, and the transaction was designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

- a. September 26, 2018 - \$2,623.64, including fees, via World Remit to Conspirator 6 in Tamale, Ghana

31. According to an interview with Person 10, whose identity is known to the affiant, Person 10 met a female on social media and was the victim of an internet scam. The female asked Person 10 to send her money to assist her returning to the United States. Person 10 estimates that he sent \$8,000 at the female's request. Person 10 eventually realized he had been scammed.

32. Bank records show that on September 27, 2018, Person 10 wired \$3,200 to Ibrahim at Huntington Bank account # xx5884. The funds received from Person 10 were commingled with funds from other sources. Using the commingled funds on or about the date set forth below, Ibrahim engaged in a financial transaction involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Simultaneously, Ibrahim transmitted the proceeds of wire fraud to a place outside the United States, and the transaction was designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

- a. September 28, 2018 - \$2,574.34, including fees, via World Remit to Conspirator 5 in Tamale, Ghana

33. Bank records show that on October 1, 2018, Person 8 wired \$25,000 to Ibrahim at Huntington Bank account # xx5884. The funds received from Person 8 were commingled with funds from other sources. Using the commingled funds on or about the dates set forth below, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Simultaneously, Ibrahim transmitted the proceeds of wire fraud to a place outside the United States, and such transactions were designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

- a. October 2, 2018 - \$2,432.92, including fees, via World Remit to Conspirator 5 in

Tamale, Ghana

- b. October 4, 2018 - \$1,733.92, including fees, via World Remit to Conspirator 5 in Tamale, Ghana

34. Bank records show that on October 5, 2018, Person 9 wired \$1,500 to Ibrahim at Huntington Bank account # xx5884. The funds received from Person 9 were commingled in the account with other funds, including those received from Person 8. Using the commingled funds on or about the dates set forth below, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Simultaneously, Ibrahim transmitted the proceeds of wire fraud to a place outside the United States, and such transactions were designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

- a. October 9, 2018 - \$1,081.68, including fees, via World Remit to Conspirator 5 in Tamale, Ghana
- b. October 9, 2018 - \$3,232.01, including fees, via World Remit to Conspirator 3 in Tamale, Ghana
- c. October 9, 2018 - \$1,077.67, including fees, via World Remit to Conspirator 5 in Tamale, Ghana

35. Bank records show that on October 10, 2018, Person 9 wired \$7,000 to Ibrahim at Huntington Bank account # xx5884. Bank records also show that on October 11, 2018, Person 10 wired \$5,000 to Huntington Bank account # xx5884. The funds received from Person 9 and Person 10 were commingled in the account with other funds, including those received from Person 8. Using the commingled funds on or about the date set forth below, Ibrahim engaged in a financial transaction involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Simultaneously, Ibrahim transmitted the proceeds of wire fraud to a place outside the United States, and the transaction was designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

- a. October 12, 2018 - \$3,210.95, including fees, via World Remit to Conspirator 5 in Tamale, Ghana

36. Bank records show that between October 24, 2018 and December 31, 2018 Person 8 wired an additional \$13,000 and Person 9 wired an additional \$8,500 to Ibrahim at Huntington Bank account # xx5884. The funds received from Person 8 and Person 9 were commingled in the account with other funds and were exhausted through various means.

37. According to an interview with Person 11, whose identity is known to the affiant, Person 11 met somebody he believed to be named Albertina William on social media. After initially meeting on social media, Person 11 also communicated with William via email. William told Person 11 that she had inherited gold from her father. William convinced Person 11 to send money to various people to pay fees, expenses and taxes needed to transport the gold from

Ghana to the United States.

38. Bank records show that between January 7 and January 17, 2019, Person 11 wired \$40,000 to Ibrahim at Huntington Bank account # xx4490. The funds were commingled with funds from other sources. Using the commingled funds and on or about the dates below, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

- a. January 8, 2019 - \$4,000 transfer to Huntington Bank account # xx5844
- b. January 22, 2019 - \$25,000 transfer to Huntington Bank account # xx5844
- c. February 4, 2019 - \$4,000 transfer to Huntington Bank account # xx5844
- d. February 5, 2019 - \$8,500 transfer to Huntington Bank account # xx5844
- e. February 7, 2019 - \$1,500 transfer to Huntington Bank account # xx5844

39. Bank records show the funds transferred from Huntington Bank account # xx4490 to Huntington Bank account # xx5844 on January 8, 2019 were commingled in the account with funds from other sources. Using the commingled funds and on or about the date below, Ibrahim engaged in a financial transaction involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

- a. January 10, 2019 - \$3,867.20, including fees, via TransferWise, an international money servicing business, to Conspirator 1

40. Bank records show that the funds transferred from Huntington Bank account # xx4490 to Huntington Bank account # xx5844 on January 22, 2019 were commingled in the account with funds from other sources. Using the commingled funds on or about the dates set forth below, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds. In two of the financial transactions, Ibrahim simultaneously transmitted the proceeds of wire fraud to a place outside the United States and the transactions were designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

- a. January 23, 2019 - \$4,127.58 transfer, including fees, via TransferWise to Conspirator 1
- b. January 23, 2019 - \$457.20, including fees, via Wave to Conspirator 5, which was received in Ghanaian Cedis
- c. January 30, 2019 - \$629.00 transfer, including fees, via Wave to Conspirator 1, which was received in Ghanaian Cedis

41. According to an interview with Person 12, whose identity is known to the affiant, Person 12

was contacted by somebody he believed to be named Patricia Batch on social media. Person 12 corresponded with Batch via text messaging applications. Eventually, Person 12 fell in love with Batch. Batch asked Person 12 to send money to various people, one of whom was in Columbus, Ohio. Person 12 discovered only later that he had been scammed.

42. Bank records show that on March 8, 2019, a check in the amount of \$1,000 issued by Person 12 was deposited into Huntington Bank account # xx5844. The funds were commingled in the account with funds from other sources. Using the commingled funds on or about the dates set forth below, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Simultaneously, Ibrahim transmitted the proceeds of wire fraud to a place outside the United States, and such transactions were designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

- a. March 11, 2019 - \$134.47 transfer, including fees, via Wave to Conspirator 3, which was received in Ghanaian Cedis
- b. March 11, 2019 - \$699.00 transfer, including fees, via Wave to Conspirator 2, which was received in Ghanaian Cedis

43. Bank records show that on March 12, 2019, a check in the amount of \$1,000 issued by Person 12 was deposited into Huntington Bank account # xx5844. The funds were commingled in the account with funds from other sources. Using the commingled funds on or about the date set forth below, Ibrahim engaged in a financial transaction involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Simultaneously, Ibrahim transmitted the proceeds of wire fraud to a place outside the United States, and the transaction was designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

- a. March 13, 2019 - \$850 transfer, including fees, via Wave to Conspirator 2, which was received in Ghanaian Cedis

44. Bank records show that on March 25, 2019 and March 27, 2019, checks in the amounts of \$1,000 and \$50,000, respectively, issued by Person 12 were deposited into Huntington Bank account # xx4490. The funds were commingled in the account with funds from other sources. Using the commingled funds and on or about the dates below, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

- a. March 29, 2019 - \$6,500 transfer to Huntington Bank account # xx5844
- b. April 1, 2019 - \$3,500 transfer to Huntington Bank account # xx5844
- c. April 4, 2019 - \$5,000 transfer to Huntington Bank account # xx5844
- d. April 8, 2019 - \$33,000 transfer to Huntington Bank account # xx5844

45. Bank records show the funds transferred from Huntington Bank account # xx4490 to Huntington Bank account # xx5844 on March 29, 2019 were commingled in the account with funds from other sources. Using the commingled funds on or about the date set forth below, Ibrahim engaged in a financial transaction involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Simultaneously, Ibrahim transmitted the proceeds of wire fraud to a place outside the United States, and the transaction was designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

- a. April 1, 2019 - \$756 transfer, including fees, via Wave to Conspirator 3, which was received in Ghanaian Cedis

46. Bank records show the funds transferred from Huntington Bank account # xx4490 to Huntington Bank account # xx5844 on April 1, 2019 were commingled in the account with funds from other sources. Using the commingled funds on or about the dates set forth below, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Simultaneously, Ibrahim transmitted the proceeds of wire fraud to a place outside the United States, and such transactions were designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

- a. April 4, 2019 - \$100 transfer, including fees, via Wave to Conspirator 3, which was received in Ghanaian Cedis
- b. April 4, 2019 - \$950 transfer, including fees, via Wave to Conspirator 2, which was received in Ghanaian Cedis

47. Bank records show the funds transferred from Huntington Bank account # xx4490 to Huntington Bank account # xx5844 on April 4, 2019 were commingled in the account with funds from other sources. Using the commingled funds on or about the dates set forth below, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds. Simultaneously, Ibrahim transmitted the proceeds of wire fraud to a place outside the United States, and such transactions were designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

- a. April 5, 2019 - \$750 transfer, including fees, via Wave to Conspirator 2, which was received in Ghanaian Cedis
- b. April 8, 2019 - \$447.93 transfer, including fees, via Wave to Conspirator 2, which was received in Ghanaian Cedis
- c. April 8, 2019 - \$97 transfer, including fees, via Wave to Conspirator 3, which was received in Ghanaian Cedis

- d. April 10, 2019 - \$610 transfer, including fees, via Wave to Conspirator 3, which was received in Ghanaian Cedis

48. According to an interview with Person 13, whose identity is known to the affiant, Person 13 is 90 years old. she met somebody she believed to be named Plasse Goldman on Facebook in January 2021. Goldman told Person 13 that he was a Four-Star General serving in Afghanistan. Goldman eventually asked Person 13 to send him money to help pay student loans. Goldman instructed Person 13 to send money to Mubarik Ibrahim, who was supposedly an attorney assisting Goldman in the process. Ibrahim was supposed to send the money to a diplomat in Kabul. Richardson eventually discovered she had been involved in a scam.

49. Bank records show that between February 25, 2021 and July 13, 2021, Person 13 wired \$23,000 to Citizens Bank account # xx8906. Ibrahim had opened Citizens Bank account # xx8906 on September 25, 2020 and was the only signer on the account. The funds were commingled in the account with funds from other sources. Using the commingled funds and on or about the dates set forth below, Ibrahim engaged in financial transactions involving the proceeds of wire fraud to conceal or disguise the nature, location, source, ownership, or control of the proceeds:

- a. March 1, 2021 - \$2,500 transfer to an undetermined recipient via Cash App, a peer-to-peer money transfer service
- b. March 1, 2021 - \$1,499.99 transfer to an undetermined recipient via Remitly, an international money servicing business
- c. March 2, 2021 - \$720.55 transfer to an undetermined recipient via Remitly
- d. May 6, 2021 - \$2,500 transfer to an undetermined recipient via Cash App
- e. May 7, 2021 - \$2,500 transfer to an undetermined recipient via Cash App
- f. May 10, 2021 - \$2,000 transfer to an undetermined recipient via Cash App
- g. May 10, 2021 - \$1,930.47 transfer to an undetermined recipient via Remitly
- h. May 10, 2021 - \$1,070.51 transfer to an undetermined recipient via Remitly
- i. May 10, 2021 – a second \$1,070.51 transfer to an undetermined recipient via Remitly
- j. July 14, 2021 - \$2,400 transfer to an undetermined recipient via Cash App

50. According to an interview with Person 14, whose identity is known to the affiant, Person 14 was in the process of buying a home in late March 2022 when she received communications from Greg, a person she believed to be involved in the purchase process. Greg instructed Person 14 to wire \$343,576.33 to an account number in order to close on the purchase of the home.

Buzzetta later spoke to others involved in the transaction and discovered that Greg was an imposter, and she had been scammed.

51. Bank records show that on March 29, 2022, Person 14 wired \$343,576.33 to Citizens Bank account # xx8906. Bank records also show that on April 19, 2022, Citizens Bank returned \$339,217.77 to Buzzetta due to a “fraud recall.”

52. On January 17, 2023, Ibrahim was advised of his right to remain silent and right to counsel two different times by Special Agents with IRS-Criminal Investigation. Both times, Ibrahim acknowledged that he understood his rights. After being advised of his rights, Ibrahim provided the following information, some of which is paraphrased by the affiant, and/or made the following statements, which appear in quotes:

- a. Ibrahim communicated with individuals in Ghana who did business with people in America, but the people in America could not wire money directly to Ghana. As such, the individuals in Ghana needed Ibrahim to receive the money from the people in America.
- b. As early as 2014 or 2015, Ibrahim asked questions of the individuals in Ghana about his receipt and transmission of money on their behalf because “it wasn’t normal.” The individuals in Ghana told Ibrahim that “they had a gold business” but “(people in the United States) could not send the money straight to Africa” because “it might get blocked.”
- c. The individuals in Ghana informed Ibrahim when his accounts received wires or deposits and often sent him “receipts” showing the wires and/or deposits. Ibrahim explained that the individuals in Ghana had received the receipts from the individuals in America who had sent the wires or made the deposits because “you know, wire takes time before it hits your account, so when they send the money, they will send a receipt...so whatever they do, they take a picture and send it to them in Africa before, before I even got to know what is going on.” After Ibrahim received money, the individuals in Ghana would instruct Ibrahim about what to do with the money. Some of the instructions included buying cars, withdrawing cash or sending money to various recipients in Ghana via money servicing businesses. Ibrahim then sometimes took pictures of his “receipts” and sent the images to the individuals in Ghana. These communications occurred on Ibrahim’s cell phone via WhatsApp. In fact, according to Ibrahim, “The majority of the communication was in WhatsApp.” Ibrahim believes the individuals in Ghana may have also instructed the individuals in America to communicate with them and send the receipts via WhatsApp. I know from investigative experience that WhatsApp is an encrypted text messaging application used by individuals to send text messages and file attachments, including photos, audio files, video files, documents, Portable Document Format files (PDFs), and other file types.
- d. When asked why the banks and money servicing businesses would stop and/or limit wire transfers, Ibrahim stated, “*Even the real businesses* (emphasis added by

affiant)...if you continue doing it consecutive times, the bank going to suspect something.” This statement indicated to the affiant that Ibrahim knew he was not involved in a “real business.”

- e. At least two of Ibrahim’s banks recalled and returned wires and told him that the wires were fraudulent. Ibrahim stated, “Huntington, they stopped, yeah, they stopped a lot of transfers.” Ibrahim also stated, “Yeah, JP Morgan, yeah, it got to a time, they closed the account. They said, uh, they said, uh, they suspected my account to be fraudulent and they said they could not do business with me no more...They said there was, uh, there was too many, um, suspicious activities in my account.” Notably, the account held at JP Morgan Chase was closed by the bank in March 2015. These statements indicated to the affiant that Ibrahim knew as early as 2015 and was reminded multiple times that the activity occurring in his bank accounts was not legitimate.
- f. Ibrahim stated that World Remit, a money servicing business, also barred him from using the service. Ibrahim stated, “Yeah, World Remit, yeah...you know I sent a lot of money...I sent a whole lot of money...so they cannot, so they think, um, its fraud, so they too, they barred me.” Notably, between March 2016 and January 2019, Ibrahim sent at least \$171,000 to various recipients in Ghana.

Technical Background

53. Based upon my training and experience, I use the following technical terms to convey the following meanings:

- a. Cell Phone/Mobile Device: A cell phone is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include

various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. **GPS:** A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. **PDA:** A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

54. Based upon my training, experience and research, I know that the devices for which the warrants are requested have capabilities to allow them to serve as a cell phone, digital camera, portable media player, GPS navigation device and PDA.

55. I have consulted with IRS-CI Special Agent-Computer Investigative Specialist Ebenger-Balla regarding the aspects of properly retrieving and analyzing electronically stored digital data. Special Agent Ebenger-Balla has been employed with IRS-CI since 2009. In addition to attending training in financial investigation techniques and accounting, she also completed the IRS-CI Basic Computer Evidence Recovery Training class at the Federal Law Enforcement Training Center in Glynco, Georgia, (2016) and the Advanced Computer Evidence Recovery Training class at the CyberCrimes Center in Fairfax, Virginia (2017), and Macintosh Forensics Training in Glynco, Georgia (2017). Special Agent Ebenger-Balla also completed the Mobile Device Forensics Training in Glynco, Georgia (2017) where she learned about the operation of mobile devices and the correct procedures for seizing and analyzing those devices.

56. Based upon the affiant's knowledge, training, experience and consultation with Special Agent Ebenger-Balla, the affiant knows that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

57. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium

58. The affiant knows that searching and seizing information from computers and cell phones often requires agents to seize most or all electronic storage devices to be imaged and searched later by a qualified computer specialist in a laboratory or other controlled environment. This requirement is due to the following:

- a. Technical requirements: Searching computer systems, such as cell phones, for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis. Further, such searches often require the seizure of most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.
- b. The volume and nature of electronic evidence: The volume of evidence. Computer storage devices such as cell phones can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

59. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

Conclusion

60. Based on the information presented in this affidavit, I contend that Ibrahim conspired to commit money laundering in violation of 18 U.S.C. § 1956(h). I further contend that Ibrahim committed multiple acts in violation of 18 U.S.C. § 1956(a)(1)(B)(i) and 18 U.S.C. § 1956(a)(2)(B)(i) in furtherance of the conspiracy. I further believe that Ibrahim and others used various cell phones to communicate regarding and to facilitate the laundering of funds derived from fraud schemes, and evidence of these violations, as well as violations of 18 U.S.C. § 1343, is now located in the item described in Attachment A. Because this warrant seeks only permission to examine device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.



Shawn A. Mincks
Special Agent, IRS-CI

Subscribed and sworn to before me

This 2nd day of February, 2023.



THE HONORABLE CHELSEY M. VASCURA
United States Magistrate Judge

ATTACHMENT A

The property to be searched is a red iPhone cell phone seized during the arrest of Mubarik Ibrahim on January 17, 2023.

Hereinafter, this cellular phone will be referred to as “the Device.” The Device is currently located at 401 North Front Street, Suite 375, Columbus, Ohio.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that are evidence of violations of Wire Fraud, in violation of 18 U.S.C. § 1343; Money Laundering Conspiracy, in violation of 18 U.S.C. § 1956(h); and Money Laundering, in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and/or 18 U.S.C. § 1956(a)(2)(B)(i); for the period December 1, 2014, to the present, including:
 - a. Records related to the wire-fraud schemes and money-laundering scheme described in the Affidavit;
 - b. Records identifying the establishment, ownership, operation and/or control of any limited liability corporation or other business entity including articles of organization; correspondence with and/or submissions to/from any Secretary of State office; applications, disposition records and/or correspondence related to the issuance or use of Employer Identification Numbers (EIN); minutes and other official business records; and documents identifying any registered agent(s), incorporator(s), and/or other identified members;
 - c. All records related to or referencing electronic transfers of funds or cash deposits including requests for an electronic transfer or cash deposit, wiring or deposit instructions, receipts, and correspondence;
 - d. All records related or referring to persons or entities in other countries and the locations of such persons or entities;
 - e. Asset ownership and/or acquisition records including contracts, invoices, receipts, registrations, titles insurance records and/or photographs of assets including motor vehicles, real property, boats, jewelry, precious metals and gems, and currency (foreign, domestic, or virtual currency);
 - f. Travel records including travel directions, hotel reservations, rental car reservations, airplane reservations, invoices, airline tickets, and itineraries;
 - g. Records related to banking activity including communications and data related to the opening, closing, use, custody and/or control of bank accounts, alternative currency accounts (i.e. those related to Bitcoins), credit cards, and/or debit cards including applications for accounts; approval or declination notices; credit and/or debit card issuance notices; credit and/or debit card activations; bank statements; welcome or account opening/closing notifications; deposit, payment, withdrawal, or transfer orders, receipts and/or notifications; balance inquiries and/or notices; and security notifications;
 - h. All financial statements, accounting records and supporting source documents relating to receipts, expenditures, general ledgers, accounts and notes receivable,

accounts and notes payable, balance sheets, income statements, statements of profit and loss, and any other accounting records and other records and/or ledgers relating to Mubarik Ibrahim or any variation of this name and any other entities identified through items seized pursuant to section a. above;

- i. Records pertaining to any financial institution account including but not limited to account numbers, passwords, personal identification numbers (PINS), deposit/withdrawal records, notes, logs, and photographs;
 - j. Electronic records of internet sites visited and data accessed and/or communications made in the course of visiting such internet sites;
 - k. Communications records and histories made through and/or from applications (known as "Apps"); emails; texts; calls or other media contained on the electronic devices to be searched and all attachments included in such communications; and
 - l. Contact lists and any documents reflecting names, addresses, email addresses, telephone numbers, fax numbers and/or other contact information.
 - m. Evidence indicating the cell phone owner's or user's state of mind as it relates to the crimes under investigation.
2. Evidence of user attribution showing who used or owned the cell phone at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.